AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A method for an authentication process within a distributed data processing system, the method comprising:

receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

2. (Original) The method of claim 1 wherein the controlled resource is a legacy application.

3. (Original) The method of claim 1 wherein the authentication data comprises a user identity and a password.

4. (Original) The method of claim 1 further comprising:

authenticating the client for access to the controlled resource based on the authentication data.

5. (Original) The method of claim 1, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the host.

6. (Original) The method of claim 1 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

7. (Original) The method of claim 1 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

8-13. (Canceled)

14. (Previously Presented) An apparatus for performing an authentication process within a distributed data processing system, the apparatus comprising:

receiving means for receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting means for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host;

and forwarding means for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

15. (Original) The apparatus of claim 14 wherein the controlled resource is a legacy application.

16. (Original) The apparatus of claim 14 wherein the authentication data comprises a user identity and a password.

17. (Original) The apparatus of claim 14 further comprising:

authenticating means for authenticating the client for access to the controlled resource based on the authentication data.

18. (Original) The apparatus of claim 14, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the apparatus further comprising:

first parsing means for parsing the authentication data to retrieve a specific set of authentication data for the host.

19. (Original) The apparatus of claim 14 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the apparatus further comprising:

second parsing means for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

20. (Original) The apparatus of claim 14 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

21-24. (Canceled)

25. (Previously Presented) A computer program product in a computer readable medium for use in a distributed data processing system for performing an authentication process, the computer program product comprising:

instructions for receiving an attribute certificate from a client at a host within the distributed data processing system;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

instructions for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

instructions for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

26. (Original) The computer program product of claim 25 wherein the controlled resource is a legacy application.

27. (Original) The computer program product of claim 25 wherein the authentication data comprises a user identity and a password.

28. (Original) The computer program product of claim 25 further comprising:

instructions for authenticating the client for access to the controlled resource based on the authentication data.

29. (Original) The computer program product of claim 25, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the host.

30. (Original) The computer program product of claim 25 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

31. (Original) The computer program product of claim 25 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

32-35. (Canceled)